Cyber Offsensive Session: Pushing the Boundaries and Action Against Hacktivism

NAME REDACTED - Serious Crime Effects, GCHQ

NAME REDACTED

- JTRIG, GCHQ



Why do an Effects Operation?

- Disruption v Traditional Law Enforcement
- SIGINT discovered the targets
- Disruption techniques could save time and money

Hacktivism: Online Covert Action

- Hacktivist groups
- Online Humint
- Effects Operations

Hacktivist groups

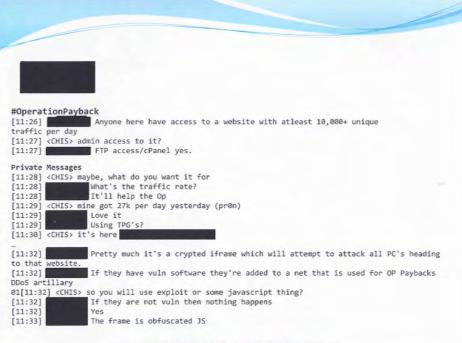
- They are diverse and often have multiple, varied aims
- Anonymous
- LulzSec
- A-Team
- Syrian Cyber Army
- Targets include: Corporations, banks, governments, copyright associations, political parties
- Techniques: DDoS, data theft SQLi, social engineering
- Aims:

Online HUMINT -CHIS

- 2 Examples from Anonymous IRC Channels:
 - Gzero
 - P0ke

Gzero &

- Asking for traffic
- Engaged with target
- Discovered Botnet with malware analysis & SIGINT
- Outcome: Charges, arrest, conviction



GZero

```
[15:16] <GZero> yo
[15:16] (GZero) works with me
[15:16] <GZero> i need traffic
[15:16] <CHIS> hev.
                                                   Infrastructure
[15:17] <CHIS> what for?
                                                   WHOIS: gzero
[15:17] <GZero> exploit pack
[15:17] (GZero) will pay you if traffic is good
[15:17] <GZero> u wanna talk?
[15:18] <GZero> http://alpha.b0x.su/hits.txt - Need to make this bigger ;)
[15:19] <GZero> http://pastebin.com/ - JS for iframe
[15:19] <GZero> http://alpha.b0x.su/iqjtcoxo8.php Live URL 1st Stage implant:
[15:19] (GZero> U have traffic?
                                                           Lead to 2nd stage & WARPIG
[15:21] <CHIS> so what is at that page anyway?
                                                           botnet, SpyEye malware
[15:21] <GZero> several exploits
[15:21] <CHIS> yeah I've got traffic. got 92k hits yesterday.
[15:22] <GZero> ok
[15:22] <GZero> lets talk :p
```

Online Humint - Gzero

- JTRIG & SIGINT reporting lead to identification, arrest
- Sentenced for 2 years April 2012

Hacker jailed for stealing 8 million identities

St. Earl Destricted / State & 1917 11-17 care Stiff

Summary: A British hacker has been sentenced to 26 months for stealing 200,000 PayPal accounts, 2,701 bank card numbers, as well as 8,110,474 names, dates of birth, and postcodes of U.K. residents.

23-year-old Edward Pearson of York, Northern England, will spend two years and two months behind bars for his hacking spree. The sentence would have been greater if he made more use of the huge amount of stolen data.

The British hacker used the Zeus and Spu'se Trojans to stead confidential data from U.K. vicins between Jaruary 1, 2010, and Jargust 30, 2011, from an undiscided source. On this computers, police found 200,000 stolen PayPal accounts, Z.701 bank card numbers, as well as 9, 100.474 names, dates of birth, and postcodes of U.K. residents. If all the details of nath the had harvared oner prired out, it would \$11 67,500 double-sided A4 pages, according to authorities.



p0ke

- Discussing a database table labelled 'FBI', in Anon Ops IRC
- Engaged with target exploiting US Government website,
 US company website

#OperationPayback

- [19:40] <&pθke> Topiary: I has list of email:phonenumber:name of 700 FBI tards
- [19:40] <&p0ke> :P
- [19:41] <Topiary> what about passwords?
- [19:41] <&p0ke> It was dumped from another gov db, Topiary
- [19:41] <&p0ke> A table named fbi
- [19:42] <Topiary> ah, like an FBI affiliated contact userbase?
- [19:42] <&p0ke> that was all it contained D:

p0ke

Private Messages

[20:04]

so what was the site?!

P0ke - Identification

Private Messages

oh btw have you seen this

[21:08] <p0ke> sexy

cool huh? [21:09]

[21:11] <p0ke> Ya

BBC Who loves the hacktivists?

... Enabled SIGINT

POke:

Name:

Facebook, email accounts

Effects on Hacktivisim

- Op WEALTH Summer 2011
 - Intel support to Law Enforcement identification of top targets
 - Denial of Service on Key Communications outlets
 - Information Operations

DDoS

- ROLLING THUNDER
 - RT initial trial info

[15:40] srewder> hello, was there any problem with the irc network? i wasnt able to connect the past 30 hours.

[15:42] <speakeasy> yeah

[15:42] <speakeasy> we're being hit by a syn flood

[16:44] <speakeasy> i didn't know whether to quit last night, because of the ddos

- anon_anonz Anonymous
 irc anonops li tango down :(
- anon_anonz Appropries
 720pHighDefenition (notice the typo) on YouTube anon_anonz on
 twitter nickname: meowitude
- anon_anonz anonmous irc. anonops.li back up @anonops #anonymous #antisec

10 Outcome

- CHIS with
- 80% of those messaged where not in the IRC channels 1 month later

Conclusion

- Team working SIGINT, JTRIG, CDO, INOC was key to success
- Online Covert Action techniques can aid cyber threat awareness
- Effects can influence the target space